IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**Crim. No. 19-88**
	:	
NATHAN STEWART WEYERMAN	:	

Diamond, J. **MEMORANDUM** **January 3, 2020**

Defendant Nathan Weyerman raises a novel challenge to the Government's emerging method of investigating child pornography trafficking on the Freenet file sharing Network. Weyerman argues that the FBI lacked probable cause to search his apartment because the Agency relied in part on an unreliable Algorithm that revealed he had retrieved child pornography from the Network. I will deny Defendant's Motion to Suppress, both because abundant probable cause supported the search, and because the Government relied in good faith on a valid search warrant.

I. PROCEDURAL HISTORY

On September 13, 2018, Magistrate Judge Marilyn Heffley issued the search warrant that Defendant challenges here. (Ex. A to Def.'s Motion to Suppress, Doc. No. 22.) As described in the warrant's supporting affidavit, between September 2017 and February 2018, the FBI learned of four attempted transmissions of Freenet files to the same user. (Probable Cause Aff. ¶¶ 31–35.) The Agency used a publicly available encryption code to obtain and then examine the files; all contained child pornography. (Id. ¶¶ 32–35.) Employing the Algorithm, the Agency determined that the user had downloaded the files. (Id. ¶ 31.) FBI Agent Rebecca Quinn then served administrative subpoenas on Verizon, the user's internet service provider, and learned that the Freenet user was Defendant. (Id. ¶ 38.) Agent Quinn prepared a search warrant and supporting 25-page affidavit detailing her training and experience, the FBI's investigation (and use of the

Algorithm), and Defendant's status as a registered sex offender (based on his 2005 conviction for raping a child). (See generally id.) Once Judge Heffley approved the warrant—which authorized the search of Defendant's apartment for materials and devices by which child pornography could be downloaded and stored—the FBI recovered child pornography videos and images from Defendant's computers, thumb drive, and external hard drive. (See Doc. No. 1.)

On February 7, 2019, the grand jury charged Defendant with receiving and possessing child pornography. (Id.); 18 U.S.C. §§ 2252(a)(2), (b)(1), (a)(4)(B) & (b)(2).

In moving to suppress, Defendant ignores most of the evidence discussed in the Quinn Affidavit, challenging only the reliability of the Algorithm. Accordingly, during the suppression hearing both Parties focused on the Algorithm. The Government called Agent Quinn and computer science and forensics expert Brian Neil Levine, Ph.D, who created the Algorithm. After the hearing, both Parties submitted proposed findings and conclusions. (Doc. Nos. 39–41.)

II. FINDINGS OF FACT

Defendant does not dispute the credibility of Agent Quinn or Professor Levine, both of whom I credit. I find that the Government has proven the following facts—almost all of which are also undisputed—by a preponderance of the evidence. Fed. R. Crim. P. 12(d); United States v. Lowe, 791 F.3d 424, 432 n.4 (3d Cir. 2015).

Freenet Overview

Since 2011 "law enforcement has been investigating the trafficking of child pornography on Freenet," an anonymous, peer-to-peer file sharing Network. (Probable Cause Aff. ¶ 25.) There are some 2,000 to 6,000 users on the Network at any time. (Def.'s Proposed Facts ¶ 2, Doc. No. 39.) Although Freenet client software is publicly available and legal to own, the Network itself is often used for storing and disseminating child pornography. (Ex. C to Def.'s Motion to Suppress,

Levine et al., Statistical Detection of Downloaders in Freenet, at 1, 7 (some 35% of Freenet traffic involves child pornography); 11/22/19 Tr. at 48:3.)

Freenet connects each user (or "node") directly to others operating Freenet software; these are the user's "peers." (Probable Cause Aff. ¶ 14 & n.2.) A user can see his peers' IP addresses, the number of peers each has, and each peer's Network "location" (a random number assigned to a user), but he knows nothing about Freenet nodes to which he is not directly connected. (Id. ¶ 25.)

Users select for themselves the number of peers to which they connect. (11/22/19 Tr. 63:19–20; Probable Cause Aff. ¶ 14 n.2.) Most connect to at least 30 peers. (11/22/19 Tr. 63:19–20.) Once the user sets the number, Freenet selects the peers based on Network location. (Id. at 14:13–15:6; Probable Cause Aff. ¶ 27.)

Encryption and Storage

Files exchanged on Freenet are encrypted and divided into 32 kilobyte blocks, which are distributed across the Network. (Levine et al., supra, at 2; 11/22/19 Tr. at 72:18–73:2.) The number of blocks into which a file is broken thus depends on its size. (See 11/22/19 Tr. at 67:5–68:3.) For instance, video files are usually much larger than image files, and so comprise more blocks. (Id. at 67:1–20.)

Each Freenet user provides hard-drive space and bandwidth to enable the Network's decentralized file storage and exchange. (Levine et al., supra, at 2.) Because Freenet files are encrypted, a user seeking to download a particular file must obtain the associated "manifest key," (a unique, lengthy series of numbers, letters, and symbols). (Id.; 11/22/19 Tr. at 10:7–22.) Freenet returns a manifest key to the user when he uploads a file to the Network. (11/22/19 Tr. at 10:23–11:8.) These keys are posted on Freenet messaging boards, Freesites, and other publicly accessible

places. (Probable Cause Aff. ¶ 27.) The labels that users append to child pornography keys are often distressingly clear ("boyporn," "pedomom," "kidfetish," "hurtcore," "tor-childporn," etc.); some posts include descriptions of the associated videos and images. (Id. ¶ 23.) Through these postings, collectors "share" access to child pornography files stored on the Network. (11/22/19 Tr. at 10:23–11:8; Levine et al., supra, at 4.)

Since 2011, police have recovered numerous manifest keys and examined the corresponding files, many of which contained child pornography. (Probable Cause Aff. ¶¶ 25, 27.) In this way, law enforcement has identified keys that are used for the storage and retrieval of child pornography. (Id. ¶¶ 26–27; Opp'n to Suppression, Doc. No. 26, at 4–5.)

Freenet is a closed system: users may access only files uploaded to the Network. (11/22/19 Tr. at 10:3–4.) Because the files are divided into constituent blocks, when a user seeks to download a file, his Freenet software requests the blocks from his peers. (Probable Cause Aff. ¶ 17; 11/22/19 Tr. at 13:10–14:9.) If the user's peer does not have the requested blocks, the peer's Freenet software automatically relays the request to his peers. (11/22/19 Tr. at 16:2–6.) This chain continues until the blocks are retrieved. Freenet assigns each request a "lifespan"—a "Hops to Live" number. (Probable Cause Aff. ¶ 18.) Because requests would otherwise ping endlessly among users, the HTL number is "decremented" by 1 with each relay. (11/22/19 Tr. at 17:10–18:3.) The request "fails"—terminates and is returned unfulfilled—once the HTL reaches 0. (Id.) Freenet has set 18 as the default HTL. (Id. at 17:19–20, 49:13–15; Probable Cause Aff. ¶18.)

File Retrieval

Freenet repeatedly "warns its users . . . that it does not guarantee anonymity." (Probable Cause Aff. ¶ 21.) Freenet also admonishes that "it can be statistically shown that a particular user more likely than not" is an original file requester. (Id.) Moreover, because an original requester's

HTL is 18, a recipient of a request with HTL 18 would know: that his peer is the original requester (and not someone relaying another user's request); the peer's IP address; and the peer's Network location. (Id.) To enhance anonymity, Freenet randomly and automatically decrements 50% of original requests to HTL 17. (Id. at 17:23–18:3; see id. at 18:21–19:8. ("And so since [anonymity is] the goal, it can't simply start everything with 18. It would be too easy to reverse that anonymity, as they call it.").) A request with an HTL of 17 thus may be a relayed request, or it may be an original request that was "initially decremented." (Probable Cause Aff. ¶ 19.) A request with an HTL 16 or lower is necessarily a relayed request. (11/22/19 Tr. at 20:17–23.)

Investigative Efforts

Since 2011, law enforcement agencies have maintained a Freenet "node" through which they seek to identify child pornography traffickers. (Probable Cause Aff. ¶ 25; Becker et al., Black Ice: The Law Enforcement Freenet Project, Ex. B to Doc. No. 22, at 10.) To its peers, the law enforcement node is like any other: it receives, fills, and relays requests for file blocks. (11/22/19 Tr. at 57:3–25.) The node differs in one key respect: it automatically logs information from each peer (i.e., IP address; number of peers; Network location) making a request for blocks. (Id. at 57:10–11, 20–25; Probable Cause Aff. ¶ 25.) The law enforcement node does not target particular users. (Probable Cause Aff. ¶ 26.) Like other nodes, its peers are automatically assigned based on Network "location," and it can collect information about only those peers. (Id.) As I have described, police also use their node to collect publicly posted manifest "keys associated with suspected child pornography files." (Id. at ¶ 27.)

Professor Levine's Expertise

Through its node, law enforcement investigates Freenet users who request files that have manifest keys associated with child pornography files. (Levine et al., supra, at 1, 7.) Police apply

the Algorithm to the Freenet data thus collected to determine whether a request for child pornography files is an original or relayed request. (Probable Cause Aff. ¶ 29; 11/22/19 Tr. at 32:6–34:19.) An original requester is necessarily downloading child pornography. (11/22/19 Tr. at 18:21–19:8.)

This methodology was introduced in a 2017 peer-reviewed, academic paper authored by Professor Levine and others. (Levine, Liberatore, Lynn & Wright, Statistical Detection of Downloaders in Freenet, Ex. C. to Defendant's Motion to Suppress, Doc. No. 22; 11/22/19 Tr. 24:11–15.) Dr. Levine is a full Professor at the at the University of Massachusetts's College of Information and Computer Sciences, where he also directs the UMass Cybersecurity Institute. (Levine CV, Ex. A; 11/22/19 Tr. at 5:11–19, 6:23–7:15.) His academic specialty is internet networks, focusing on privacy, security, and forensics. (11/22/19 Tr. at 4:16–18.)

Professor Levine testified at suppression without objection as a computer science and forensics expert. (Id. at 8:8–23.) Having closely studied Freenet, Professor Levine explained with minimal jargon the Network's general structure, and described his development of the Algorithm the FBI employed here.

The Levine Algorithm

As I have discussed, Freenet requires an original requester to retrieve a specific number of blocks to "complete" (i.e. successfully download) the file he seeks. (11/22/19 Tr. at 25:20–26:3.) The original requester will thus seek that specific number of blocks distributed across his peers. (Id. at 29:5–30:12.) If he needs 1,000 blocks to complete a file and has 10 peers, the original requester will issue 100 requests for blocks to each peer. (Id.) If a peer is unable to fill the 100 requests, he would then divide and relay them to his peers. (Id. at 29:16–20.) These latter "two-hop" peers—who are removed from the original requester by a relayer—would thus receive 10

requests, far fewer than the 100 received by the original requester's adjacent node. (Id. at 29:21–23.)

"[I]f a user has a small number of peers, and forwards a request to one of those peers, the number of requests to each peer may appear high, even when the user is not the original requester." (Def.'s Proposed Conclusions of Law, Doc. No. 39, ¶ 11, Doc. No. 39; see Tr. 65:15–22.) Because reducing the number of peers limits the user's ability to request and retrieve data—thus defeating Freenet's primary purpose—such reductions are quite unusual. (Tr. 63:25–64:1–22.)

In Professor Levine's test Model, original requesters necessarily request a greater number of blocks than a user two or more hops away. (Tr. 36:12–38:3; Levine et al., supra, at 7 fig.2.) This was confirmed when the Professor and his colleagues took 10,000 samples across four distinct Network configurations. (Levine et al., supra, at 7 & fig.2.) The Model accounts for differences in file sizes. (11/22/19 Tr. at 66:17–20.) The Model operates under the extremely conservative assumption that each user has only 8 peers. (Id. at 79:15–80:6.) To facilitate Network searches and storage, however, that figure is invariably closer to 30. (Id. at 79:15–80:6.) Indeed, Defendant had over 40 peers. (Id. at 81:12–13.)

The Levine Model considers only requests with an HTL of 18 or 17. (Levine et al., supra, at 7.) It is thus limited to requests that—based on default Freenet settings—must be either original or two-hop requests. (11/22/19 Tr. at 28:15–19; Levine et al., supra, at 7.) Extending the Model to lower number HTLs would include requests that necessarily are not original. (Levine et al., supra, at 8.)

The Algorithm's Accuracy

The Model is approximately 98% accurate: in 2% of the simulations, the Algorithm mistakenly deemed a request from a two-hop node as original. (Id. at 7; 11/22/19 Tr. at 31:23–

32:4.) Between November 2016 and January 2017, Professor Levine and his co-authors also tested their Algorithm in practice by operating their own Freenet nodes (which function similarly to the law enforcement node) and collecting request data. (Id. at 7.) They applied the Algorithm to requests with HTLs of 16 or below. (Id. at 8.) Because these requests are necessarily from relayers, if the Algorithm deemed any such request as original, this would be a "false positive." (Id.) The researchers collected 26,963 requests over six weeks; the Algorithm mistakenly identified only 323 as original, reflecting a false positive rate of 1.2%. (Id.) Making a further conservative adjustment, they revised the false positive rate to 2.3%. (Id.) Again, the finding is based on "actual requests that [the researchers] received on the real network . . . [where they] get to observe what actually happens." (11/22/19 Tr. at 45:5–12.)

Since their paper's 2017 publication, Professor Levine and his colleagues have refined their approach. (Id. at 33:14–34:15.) For instance, they have tested the Model by observing the law enforcement node's interactions with another passive node connected to Freenet. (Id. at 33:16–20.) This passive node never sends original requests; it only relays its peers' requests. (Id.) Once again, if the Algorithm deems a request from this passive peer as original, that is necessarily a false positive. (See id. at 33:20–24.) Of the 465 times that "investigators have come across this node," they have without exception concluded it was a "relayer"—100% accuracy. (Tr. 33:25–34:6.)

Rewriting Freenet to Defeat the Algorithm

Freenet is "open source": the underlying code is available on the internet. (Id. at 48:4–9.) It is thus theoretically possible to rewrite the source code and change a user's HTL to a number other than 18. (Id. at 49:16–19.) In practice, however, this would be exceedingly difficult. (Id. at 51:10–14, 76:10–11.) The Freenet source code is a huge document that would comprise some 1,000 pages in hard copy. (Id. at 52:21–53:2.) Rewriting this "very complicated program" would

require numerous changes to disparate parts of the source code, which is itself poorly organized and has no "table of contents." (Id. at 52: 9–13.) Such changes could be made only by someone with significant computer science training. (Id. at 51: 8–13 ("I'm just estimating, Your Honor . . . maybe one or two semesters of computer science college courses.").) I thus credit Professor Levine's uncontradicted testimony that such changes, although theoretically possible, do not impugn the Algorithm's reliability. (Id. at 51:25–52:1.)

The difficulty of rewriting Freenet aside, one user's modification alone cannot defeat the Algorithm. (See Tr. at 60:16–21.) If an original request is sent with an HTL of 20, for example, the recipient will nonetheless decrement it to 18 if the recipient's software is unmodified. (Id.) One user's modification thus has no effect on other users. (Id. at 60:16–23, 61:16–19.) To change Freenet's default HTL of 18, both the original requester and recipient (whose actual identity is unknown to the original requester) must have rewritten the Freenet source code in exactly the same way—something even more unlikely than a single user's successful modification. (Id. at 61:3–19 ("These are all possibilities. However, again, that's the purpose of the other test. To the extent that these [modifications] are possible, yes. Do we observe them in practice? No.").)

The Instant Investigation

Between September 2017 and February 2018, Agent Quinn observed that on four occasions, requests for large numbers of blocks for files with a manifest key associated with child pornography were transmitted from the computer of a single user. (Probable Cause Affidavit ¶¶ 32–35.) Using the key, the Agent retrieved and examined the files, all of which contained child pornography. (Id.) Applying the Levine Algorithm, Agent Quinn determined that this user was downloading the files: that he was an original requester (and not merely a relayer). (Id. ¶ 31.) Agent Quinn knew from her experience that collectors of child pornography "almost always"

retain copies of the pornography "in the privacy and security of their homes," often on computers and related devices. (Id. ¶ 10(c).) She served an administrative subpoena on Verizon—the user's internet service provider—and learned that the user's IP address was subscribed in Defendant's name at his girlfriend's Philadelphia residence: 5994 Tackawanna Street. (Id. ¶¶ 37–38.) After determining from public databases that Defendant's Philadelphia residence was 1625 Dyre Street, Apartment D, the Agent served a second administrative subpoena on Verizon and learned that internet service at the apartment was also subscribed in Defendant's name. (Id. at ¶¶ 39–40.) Investigators further learned that Defendant had registered as a prior sex offender at his Dyre Street address, that he was still on parole for his 2005 child rape conviction, and that he visited his girlfriend at the Tackawanna Street address. (Id. at ¶ 41.)

Agent Quinn prepared a search warrant for each address. Both warrants were supported by the same affidavit. After Judge Heffley approved the warrants, the FBI searched the residences of Defendant and his girlfriend. (Opp'n to Suppression at 2–3.) Agents recovered from the laptop computer, desktop computer, and drives in Defendant's apartment child pornography video and image files that Defendant now asks me to suppress. (Id. at 3.) Because evidence was not recovered from the girlfriend's residence, Defendant challenges only the warrant authorizing the search of his Dyre Street apartment.

III. CONCLUSIONS OF LAW

Once again, the exclusive focus of Defendant's Motion is the Levine Algorithm. Defendant thus argues that because the Algorithm "is unreliable and subject to false results," the search warrant issued by Judge Heffley was unsupported by probable cause. (Def.'s Proposed Conclusions of Law ¶ 13.) I disagree. Without the Levine Algorithm, the evidence described in the Quinn Affidavit makes it more likely than not that Defendant was an original requester of the

child pornography files. With the Levine Algorithm, Agent Quinn established the overwhelming likelihood that Defendant downloaded the files he asks me to suppress.

In the alternative, I will deny Defendant's Motion because the Government relied in good faith on the search warrant approved by Judge Heffley.

A. The Search Warrant Comported with the Fourth Amendment

"[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." Maryland v. Pringle, 540 U.S. 366, 370–71 (2003) (quoting Illinois v. Gates, 462 U.S. 213, 232 1983) (alteration in original)). The Supreme Court has thus explained that all it requires "is the kind of 'fair probability' on which reasonable and prudent [people,] not legal technicians, act.'" Florida v. Harris, 568 U.S. 237, 243 (2013) (quoting Gates, 462 U.S. at 235 (alteration in original)). In reviewing a proposed warrant, the Magistrate Judge must thus reach a "practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . , there is a fair probability that contraband or evidence of a crime will be found in a particular place." Gates, 462 U.S. at 238. Where a lack of probable cause is alleged, the Government must prove its existence by an evidentiary preponderance. See United States v. Matlock, 415 U.S. 164, 177 n.14 (1974).

I will thus determine whether Judge Heffley "had a 'substantial basis' for concluding that the affidavit supporting the warrant established probable cause." United States v. Miknevich, 638 F.3d 178, 181 (3d Cir. 2011) (quoting United States v. Jones, 994 F.2d 1051, 1054–55 (3d Cir. 1993)). Plainly, she did.

In its 50 paragraphs, the Quinn Affidavit details the steps the Government took here, including: the FBI's investigation of Freenet since 2011; the four transmissions of large quantities of file blocks to a single user; Agent Quinn's determination that the files contained child

pornography; the FBI's extensive use and knowledge of the Levine Algorithm; Agent Quinn's determination (using the Algorithm) that the Freenet user in question was an original requester of the files; the Agent's training and experience concerning the conduct of child pornography collectors; and Verizon's confirmation that the Freenet user was Defendant. Finally, in her Affidavit, Agent Quinn notes that Defendant is a registered sex offender, still on parole for his 2005 child rape conviction. (Probable Cause Aff. ¶ 41); see United States v. Schwinn, 376 F. App'x 974, 979 (11th Cir. 2010) (statement of defendant's sex-offender status strengthened affidavit's probable cause to search for evidence of child pornography); United States v. Frechette, 583 F.3d 374, 379–80 (6th Cir. 2009) (same).

Once again, Defendant ignores the bulk of this evidence, basing his probable cause challenge entirely on his contention that the Levine Algorithm's purported unreliability. Defendant is simply incorrect.

A product of significant research and a deep knowledge of Freenet, the Algorithm is extraordinarily reliable, showing 98 to 100% accuracy in distinguishing between original requesters and relayers of Network files. This degree of accuracy compels the common-sense conclusion that Defendant was an original requester of the files he asks me to suppress. That conclusion is bolstered by the FBI's prudence in seeking a search warrant only after observing four attempted transmissions of child pornography files to the same Freenet user. Surely the likelihood is negligible that the Levine Algorithm failed repeatedly and that the same user happened to relay requests for child pornography files four times in five months (despite request characteristics indicating otherwise). The Agent's actions thus were manifestly reasonable. See Brigham City v. Stuart, 573 U.S. 373, 403 (2006) ("[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'").

Defendant presents no evidence to impugn the Levine Algorithm. Rather, Defendant raises only the theoretical possibility that a computer-educated user and his computer-educated, adjacent (anonymous) peer might, with great effort, make numerous, identical changes to their downloaded versions of the Freenet source code. This contrived invention hardly weakens Judge Heffley's probable cause finding. See Miknevich, 638 F.3d at 182 (Magistrate Judge must only find a "fair probability" that evidence of a crime will be found) (quoting Gates, 462 U.S. at 238). To the contrary, the actual evidence overwhelmingly confirms that the Levine Algorithm reliably revealed that Defendant was downloading child pornography.

In sum, it is apparent that the search of Defendant's apartment was supported by probable cause. The Government's use of the Algorithm was only a single—albeit significant—step in its investigation. Even without the Algorithm, the evidence set out in the Quinn Affidavit makes it more likely than not that Defendant possessed child pornography. See Gates, 462 U.S. at 236 ("[S]o long as the magistrate had a substantial basis for . . . conclud[ing] that a search would uncover evidence of wrongdoing, the Fourth Amendment requires no more.") (internal quotation marks and citations omitted; alterations in original). Adding the information provided by the Algorithm—with its 98 to 100% accuracy—that likelihood became a virtual certainty. Because the search warrant thus complied with the Fourth Amendment, I will deny Defendant's Motion. See United States v. Ritter, 416 F.3d 256, 262 (3d Cir. 2005).

B. The Government Acted in Good Faith

In the alternative, I will deny Defendant's Motion because the Government relied in good faith on the search warrant issued by Judge Heffley.

Courts will admit evidence obtained in violation of the Fourth Amendment, provided the law enforcement "officer execute[d] a search in objectively reasonable reliance on a warrant's

authority." United States v. Hodge, 246 F.3d 301, 307 (3d Cir. 2001) (internal quotation marks omitted). Such reliance is unreasonable only if the defendant can make a substantial showing that good faith could not have existed because of the following:

> (1) the magistrate [judge] issued the warrant in reliance on a deliberately or recklessly false affidavit;
> (2) the magistrate [judge] abandoned [her] judicial role and failed to perform his neutral and detached function;
> (3) the warrant was based on an affidavit "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; or
> (4) the warrant was so facially deficient that it failed to particularize the place to be searched or the things to be seized.

Id. at 308 (quoting United States v. Williams, 3 F.3d 69, 74 n.4 (3d Cir. 1993) (alterations in original); see, e.g., United States v. Pavuluk, 700 F.3d 651, 663–64 (3d Cir. 2012).

Defendant does not dispute the Government's good faith, or even address the issue. He thus does not suggest that the Quinn Affidavit was in the least untruthful (much less that it was deliberately or recklessly so). (11/22/19 Tr. at 83:4–7.) Moreover, as I have described, on their faces, the Quinn Warrant and Affidavit were plainly valid. The Agent limited the search of Defendant's apartment, particularizing items falling into three categories of "things to be searched or seized," all relating to possible violations of 18 U.S.C. §§ 2252 and 2252A (possession of child pornography): (1) all records and visual depictions of child pornography and evidence of communications with children; (2) telephone records; and (3) computer devices and storage media, software, and data security devices and materials. (Ex. B to Search Warrant). This list was appropriate, given the evidence that Defendant had repeatedly downloaded child pornography files from Freenet. See United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars and Fifty-Seven Cents, 307 F.3d 137 (3d Cir. 2002) ("The Fourth Amendment does not prohibit searches for long lists of documents or other items provided that . . . each item is particularly described."). Finally, Judge Heffley exercised appropriate judgment and detachment in reviewing

and approving the warrant.

In sum, because there is nothing to impugn the Government's good faith reliance on the Quinn Warrant, I will not suppress the evidence recovered from Defendant's apartment.

IV. CONCLUSION

I will deny Defendant's Motion to Suppress. Because probable cause supports the search warrant issued by Judge Heffley, there was no Fourth Amendment violation. In the alternative, I conclude that because the Government relied on the warrant in good faith, the evidence recovered during the search is admissible.

An appropriate Order follows.

/s/ Paul S. Diamond

January 3, 2020 Paul S. Diamond, J.